PERMISSIONS

When Someone Leaves, Which Access Stays?

The departure was friendly. The laptop came back and the inbox was closed. Two weeks later, a folder is still shared with a personal account and an invoicing tool still uses a credential created by the former colleague. Forgotten access does not require a dispute.

Separate the Person from What They Keep Running

Before the departure, identify work accounts, devices and automated tasks that depend on that person. Disabling an account before transferring an integration may break it. Resolve the dependency instead of using it as a reason to leave permissions in place indefinitely.

- Transfer files, calendars and responsibilities to authorised people through the company’s agreed process.
- Remove roles and review sessions, devices, connected applications and integration credentials in each service.
- Change shared credentials the person knew, and replace shared access with individual accounts where practical.
- Check public links and invitations to external accounts that could allow access without the corporate login.

Check That Removed Permissions Are Rejected

A completed checklist does not establish that every tool received the change. Use an authorised test account to verify that withdrawn permissions are rejected in the relevant places. Do not ask the departing person to surrender private credentials or enter their personal inbox.

Record who removed access and when it was checked. If anything must be retained, document its purpose, owner and retention period under the applicable policies. Human resources, operations and system administrators need to coordinate the same departure.

This review can improve the next arrival too. Assigning access by responsibility from the first day

makes it easier to know what to remove when that responsibility changes.

> *Removing permissions reduces future access but cannot erase copies already downloaded. Retention of data and communications needs its own decisions alongside the technical offboarding.*

A Check You Can Run

Consider a scheduled report created by a departing employee. Removing the account may revoke access and also stop a legitimate business task. List the task's owner, credentials and delivery destination, transfer it through the provider's supported process, and verify both outcomes: the report still runs, and the former employee no longer has the permissions being removed.

Supporting guidance: OWASP guidance on reviewing permissions.
https://cheatsheetseries.owasp.org/cheatsheets/Authorization_Cheat_Sheet.html

Continue with: Before Designing Screens, Decide Who Can Change What.
https://systems.kavaliero.com/en/blog/before-designing-screens-decide-who-can-change-what

For help with this work, see the scope of Security Audits & Penetration Testing.
https://systems.kavaliero.com/en/services/security-audits